Modeling failure cascades in critical infrastructures with physically-characterized components and interdependencies

Enrico Zio, Giovanni Sansavini

Modeling failure cascades in critical infrastructures with physically-characterized components and interdependencies

E. Zio
Ecole Centrale Paris and Supelec, Paris, France
Energy Department, Politecnico di Milano, Via Ponzio 34/3, I-20133 Milan, Italy

G. Sansavini
Energy Department, Politecnico di Milano, Via Ponzio 34/3, I-20133 Milan, Italy

ABSTRACT: In this work, the modeling of interdependent complex infrastructures (CIs) is carried out in a cascading failure simulation framework which accounts for the physical specialization of the components and their interdependencies. The analysis focuses on cascading failures triggered by the intentional removal of a single component in the CIs. The influence of the systems operating safety margins and interdependency parameters on the consequences of the cascade are assessed. A ranking of the most critical components is provided, based on the magnitude of the disruption caused by their removal.

1 INTRODUCTION

The full characterization of the vulnerability of critical infrastructures (CIs) requires modeling the dynamics of flow of the physical quantities within the network. This entails considering the interplay between structural characteristics and dynamical aspects, which makes the modeling and analysis very complicated since the load and capacity of each component, and the flow through the network are often highly variable quantities both in space and time.

Functional models are, then, often used to capture the basic features of CIs networks within a weighted topological analysis framework, i.e. disregarding the representation of the individual dynamics of the CIs elements (Motter and Lai 2002; Dobson, Carreras et al. 2007; Zio and Sansavini 2009). These models can shed light on the way complex networks react to faults and attacks, evaluating their consequences when the dynamics of flow of the physical quantities in the network is taken into account. The response behavior often results in a dramatic cascade phenomenon due to avalanches of node breakings.

As infrastructures do not exist in isolation of one another, the relations among them must be identified to perform realistic analyses (Rinaldi 2004). This shifts the focus of the research on CIs from single, isolated systems to multiple, interconnected and mutually dependent systems with the additional objective of assessing the influences and limitations which interacting infrastructures impose on the individual system operating conditions (Zimmerman 2001).

The modeling of interdependent CIs can be carried out in a cascading failure simulation framework which abstracts the physical details of the services provided by the individual infrastructures, while at the same time capturing their essential operating features and interdependencies, and examines the emergent effects of disruptions, with the associated downstream consequences (Newman et al. 2005; Zio and Sansavini 2010). Interdependencies are modeled as links connecting nodes of the interdependent systems; these links are conceptually similar to those of the individual systems and can be bidirectional with respect to the “flow” between the interdependent networks.

In this paper, such framework is extended to account for the physical nature of the components and their interdependencies. The propagation of cascading failures in a power transmission network is taken as reference example; its components are physically specialized in “generators” and “distributors”; the effects onto two interdependent CIs (communication and transportation networks) are investigated, whereby the interdependencies are modeled as “physical”, “cyber”, “geographic” and “logical” (Rinaldi et al. 2001). The analysis focuses on cascading failures triggered by the intentional removal of a single component, e.g. due to a malicious attack.

The paper is organized as follows: the modeling of cascading failures in CIs with physical characterization of components is presented in Section 2; in Section 3, the physical characterization of interdependencies is introduced; in Section 4, the functional model for interdependent CIs is detailed; in Section 5, the proposed model is applied to three interdependent CIs whose structures are based on the 380 kV Italian power transmission network (TERNA 2002, Rosato, Bologna et al. 2007). Conclusions are drawn in Section 6.

2 A MODEL OF CASCADING FAILURES IN A POWER TRANSMISSION NETWORK

The model proposed represents the power grid as a network of N nodes (substations) and K edges (transmission lines). Two types of substations are distinguished: N_G generators are the sources of power and N_D distribution substations are at the outer edge of the transmission grid, as centers of local distribution grids.

While the connectedness of the power grid allows for the transmission of power over large distances, it also implies that local disturbances propagate over the whole grid. The failure of a power line due to lightning strike or short-circuit leads to the overloading of parallel and nearby lines. Power lines are guarded by automatic devices that take them out of service when the voltage on them is too high. Generating substations are designed to switch off if their power cannot be transmitted; this protective measure has the unwanted effect of diminishing power for all consumers. Another possible consequence of power line failure is the incapacitation of transmission substations, possibly causing that the power from generators cannot reach distribution substations and ultimately consumers.

In the unperturbed state each distribution substation can receive power from any of the generators. As substations lose function, the number of generators, N_G^i, connected to (and able to feed) a certain distribution substation i decreases. The concept of connectivity loss, C_L, is used to quantify the average decrease in the number of generators connected to a distributing substation (Albert et al. 2004). The calculation of this parameter relies on the topological structure of the network and the available least-resistance pathways. Denoting by N_G the order of the generation subset at the unperturbed state of the network, and N_G^i the number of generation units able to supply flow to distribution node i after disruptions take place

$$C_L = 1 - \frac{1}{N_D} \sum_{i=1}^{N_D} N_G^i \big/ N_G \tag{1}$$

where the averaging is done over all distributing substations. In summary, the connectivity loss measures the decrease of the ability of distribution substations to receive power from the generators.

The load on a transmission or distribution substation is modeled as dependent on the number of links transiting through it, when flow is sent from each available generation node to each distribution node. In this view, the maximum load or amount of flow passing through a node is measured by the node betweenness (Sabidussi 1966; Nieminen 1974; Freeman 1978; Freeman, Borgatti et al. 1991; Little 2002), calculated as the number of shortest paths that pass through a node, when flow is sent from each available generation node to each distribution node. The node with the highest value of betweenness is that through which the most electric power flows within the system. Assuming that power is routed through the most direct path, the betweenness of a substation is a good approximation of how much power it is transmitting, i.e. its load (Albert et al. 2004).

In the proposed modeling framework, the load at a component is then the total number of shortest paths connecting every generator to every distributor passing through that component (Newman and Girvan 2004), (Batagelj 1994). At any instant of time, the load is to be compared with the component capacity, i.e. the maximum load that it can process. In man-made networks, the capacity of a component is limited by technological limitations and economic considerations. For modeling purposes, it can be assumed that the capacity C_j of component j is dimensioned proportionally to its nominal load L_j at which it is designed to operate initially,

$$C_j = (1+\alpha) \cdot L_j \quad j = 1, 2, ..., N \tag{2}$$

where the constant $\alpha > 0$, called the tolerance parameter of the power transmission network, is for simplicity assumed equal for all components. This parameter can be regarded as an operating margin allowing safe operations of the component under possible load increments. When $\alpha = 0$, the system is working at its limit capacity, its operating margin being null: any further load added to a component would result in its failure and removal from the network and in the propagation of a cascading failure involving a large part of the system.

When all the components are working, the network operates without problems in so far as $\alpha > 0$. On the contrary, the occurrence of component failures leads to a redistribution of the shortest paths in the network and, consequently, to a change in the loads of the surviving components. If the load on a component increases beyond capacity, the component fails and a new redistribution of the shortest paths and loads follows, which, as a result, can lead to a cascading effect of subsequent failures.

In the modeling scheme adopted, the distribution of loads is in turn highly correlated with the distribution of links: networks with heterogeneous distribution of links are expected to be heterogeneous with respect to the load, so that on average components with large number of links will have high loads. This behavior confirms the robust-yet-fragile property of heterogeneous networks, which was first observed in

(Albert, Jeong et al. 2000) with respect to the attack on several components.

The importance of the cascade effect with respect to intentional attacks stems from the fact that a large damage can be caused by the attack on a single component. Obviously, in general more links render a network more resistant against cascading failures, but this increases the cost of the network.

When looking at the potential of a cascading process triggered by the removal of a single component, two situations are expected: if prior to its removal the component is operating at a relatively small load (i.e., if a small number of shortest paths go through it), its removal will not cause major changes in the balance of loads and subsequent overload failures are unlikely; however, when the load of the component is relatively large, its removal is likely to affect significantly the loads of other components and possibly start a sequence of overload failures. Intuitively, the following behavior is expected (Motter and Lai 2002): global cascades occur if the network exhibits a highly heterogeneous distribution of loads and the removed component is among those with highest loads; otherwise, cascades are not expected.

3 MODELLING OF INTERDEPENDENCIES AMONG CRITICAL INFRASTRUCTURES

According to (Rinaldi et al. 2001), interdependency is a bidirectional relationship between two infrastructures by means of which the state of an infrastructure is somehow dependent on the state of another infrastructure, and vice versa. From this view interdependencies are macro-properties of coupled systems, i.e. ‘systems of systems’: they do not in general exist between individual components of systems. Other interpretations, however, do not necessarily treat interdependencies as bidirectional relationships; instead they are seen as unidirectional relationships between systems, thus treating dependencies and interdependencies as synonyms (McDaniels et al. 2007).

This view is embraced in the present work in which interdependencies among different CIs are physically specialized. Thus, the influence that infrastructure *i* exerts on infrastructure *j* is not symmetric.

In (Rinaldi et al. 2001) a classical framework for the characterizations of interdependencies is proposed. Interdependencies are characterized as either physical (an output from a system is required as an input to another system), cyber (the state of a system is dependent on information transmitted through an information infrastructure), geographic (two or more systems can be affected by the same local event, i.e. they are spatially proximate), and logical (includes all other types of interdependencies, for example related to human behavior).

Functional dependencies between infrastructures are modeled as edges between nodes in different infrastructures. If an infrastructure is not able to supply the demanded service the outgoing dependency edge is removed, thus signaling the unavailability of the desired service to other infrastructures. The effect of a removed dependency edge is evaluated separately in the functional model of each of the dependent infrastructures. This means that each infrastructure only sees and acts upon local information regarding dependencies (Johansson and Jonsson 2009).

In the following, physically specialized interdependencies among three CIs, i.e. power transmission, communication and railway networks, are modeled and analyzed.

Physical dependencies: the output of a node from a CI is required for the node in the dependent CI to operate, thus if the dependency edge is removed, the node in the dependent system is disconnected from its network.

Cyber dependencies: the output of a node from a communication network is required for the node in the dependent CI to operate safely. If the dependency edge is removed, i.e. the dependent node has no access to the communication service, it may fail and is disconnected from its network with probability p.

Logical dependencies are modeled in a similar way as the cyber dependencies.

Geographical dependencies: two or more systems can be affected by the same local event, i.e. they are spatially proximate. Nodes connected by geographical dependencies fail simultaneously when they are hit by the same local spatial event.

4 FUNCTIONAL MODEL OF INTERDEPENDENT SYSTEMS

Only the most essential functional properties of the CIs are modeled in order to provide a clear presentation of the developed methodology. More detailed functional models, embedding additional physical features, could be developed in case a more realistic characterization of the CIs is required.

The functional models of the railway and of the communication systems consist in a connectedness evaluation algorithm ascertaining the average shortest path length in the networks. The variation in the systems performances is evaluated as the relative decrease in the average global efficiency, ΔE_{glob}, with respect to the unperturbed systems (Latora and Marchiori 2005).

A node of the railway network is in service as long as it has access to the telecommunication system and as long as the power transmission system is able to supply electricity. Hence, each node of the railway network has a cyber dependency from the telecommunication system and a physical dependency from the power transmission network. If the interdependent node in the communication network fails, the node in the railway network may fail with probability p_{cr}, while if the interdependent node in the power transmission network fails, the node in the railway network is disconnected.

A node of the communication network is in function as long as the power transmission system is able to supply electricity. Hence, each node of the communication network has a physical dependency from the power transmission network. If the interdependent node in the power transmission network fails, the node in the railway network is disconnected.

The functional model of the power transmission network has been introduced in Section 2. An input from the communication system is required for the nodes of the power transmission network to operate. Hence, each node of the power transmission network has a cyber dependency from the communication network. If the interdependent node in the communication network fails, the node in the power transmission network may fail with probability p_{cp}.

From the functional descriptions of the three CIs, it follows that cascading failures only propagate in the power transmission network due to the rerouting of the flows between generators and distributors and their effects propagate to the communication and railway networks through the removal of the interdependency connections. Moreover, unlike the communication and the power transmission systems, which show mutual interdependencies, the operation of the transportation network are affected by the other two CIs but has no effect on them.

5 CASE STUDY

The model of cascading failure introduced in Section 2 has been applied to the topological network of the 380 kV Italian power transmission network (Figure 1). The 380 kV Italian power transmission network is a branch of a high voltage level transmission, which can be modeled as a network of N=127 nodes (N_G=30 generator and N_D=97 distributor nodes) connected by K=342 links (TERNA 2002, Rosato, Bologna et al. 2007). In Section 5.1, the propagation of cascading failures for the isolated independent power transmission network is assessed. In Section 5.2, two additional CIs interdependent on the power transmission network are considered, i.e. the communication network and the railway network. The effects of the interdependencies among these CIs modeled in Sections 3 and 4 have been assessed. Due to the lack of actual data but with no loss of generality, the topological structures of the two interdependent CIs have been developed on the basis of the topology of the 380 kV Italian power transmission network. Redundancies have been added to the communication network assuming that the neighborhood of each node forms a fully connected subgraph. This accounts for the presence of alternative communication routes among nodes which are not 'too far' from each other. The railway network reproduces exactly the topology of the power transmission network.

Figure 1. The 380 kV Italian power transmission network (TERNA 2002, Rosato, Bologna et al. 2007).

5.1 *Independent power transmission network*

The effects of cascading failures are first investigated in the isolated power transmission network. The scenario considered regards the malevolent targeted attack aiming at disconnecting node {88}, which handles the largest load in the system, i.e. through which pass the largest number of generator-distributor shortest paths. Previous studies have showed that power transmission networks can be very sensitive to this kind of attacks due to the difficulty of handling flow redistribution when the most congested elements fail, because neighboring elements are also working close to their full capacity and are incapable of handling significant additional flows (Duenas-Osorio & Vemuru 2009). Hence, the disconnection of a most congested node is regarded as a critical scenario of malicious attack. In addition to that, node {88} plays a strategic role in the system, bridging the northern and the southern branches of the Tyrrhenian backbone.

Once the triggering event occurs, flow redistribution takes place as a mechanism to equilibrate supply and demand constraints. The flow redistribution process is followed by introducing an artificial cascade discrete time step t_i: at t_0 the network is intact, at t_1 the initial induced failure occurs; and at $t_{\geq 2}$ the cascading failure progresses as nodes overload and cause further failures in neighboring elements. The cascading process is followed until the response stabilizes and indicators of the severity of the cascade are computed such as the cascade size S, i.e. the number of failed components, and the connectivity loss, C_L (Section 2).

In Figure 2, the final value of the connectivity loss, C_L, once the system response has stabilized, is plotted versus the tolerance parameter, α.

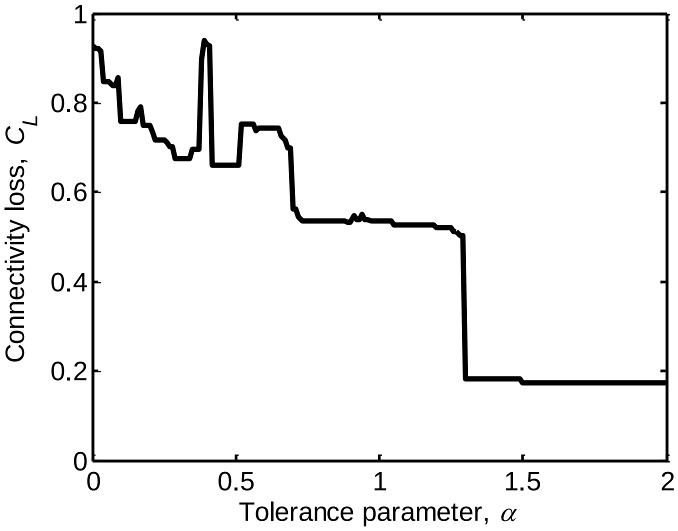

Figure 2. The final value of the connectivity loss, C_L, vs. the tolerance parameter, α, when the system response has stabilized. The cascades are triggered by the removal of the most congested node {88}.

As expected, increasing the flow-carrying capacity of the network elements reduces the extent of the cascades because flow redistribution can be handled at the local scale. Yet, we observe jumps to larger values of the connectivity loss. In order to gain a deeper understanding of this, the transition taking place at $0.34 \leq \alpha \leq 0.42$ is analyzed in detail. Figures 3 and 4 show the cascade evolution in terms of the cascade size, S, and in terms of the connectivity loss, C_L, for three values of the tolerance parameter in the range $0.34 \leq \alpha \leq 0.42$. At the second time step, S and C_L are larger for α = 0.34 than for α = 0.39, as expected. However, at the third time step, the values of S and C_L for α = 0.39 are almost three times as large as they are for α = 0.34. This behavior is related to the so-called "islanding" effect. For α = 0.34, the failures of 'weak' nodes occurring at the second time step split the network into isolated islanding sections (namely, the northern and the southern parts of the network), disconnecting many generator-distributor paths and thus reducing the demand and stabilizing the power transmission system. Conversely, for α = 0.39, nodes {71, 83, 84} along the Adriatic backbone are not failed at the second time step, allowing flow redistribution to weaker nodes, which fail subsequently at the third time step disrupting the power transmission network. This behavior suggests the inclusion of 'weak' nodes in the system design, for early disconnection or islanding and cascade-controlled operation of CIs. Finally, the sharp transition occurring at α = 0.42 (Figure 2) is due to the fact that nodes which are neighbor of high load nodes are able to handle the redistribution of flow thanks to the tolerance increase. This is the case also for the sharp transitions at α = 0.69 and α = 1.29 in Figure 2.

The effects of the physical specialization of the components in the power transmission system can be seen by comparing Figure 3 and Figure 4. Despite the larger number of components, S, failed for α = 0.42 as compared to α = 0.34, the connectivity loss, C_L, assumes higher values for α = 0.42 due to the fact that more generator-distributor paths are active in the network.

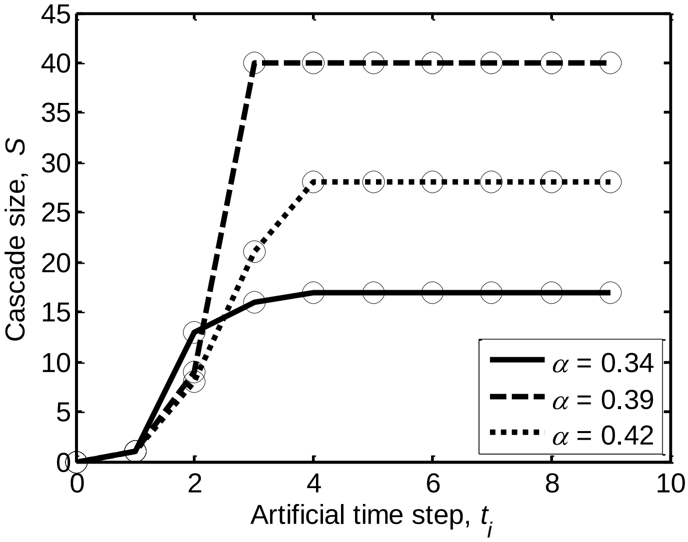

Figure 3. The cascade evolution in terms of the cascade size, S, for three values of the tolerance parameter in the range $0.34 \leq \alpha \leq 0.42$.

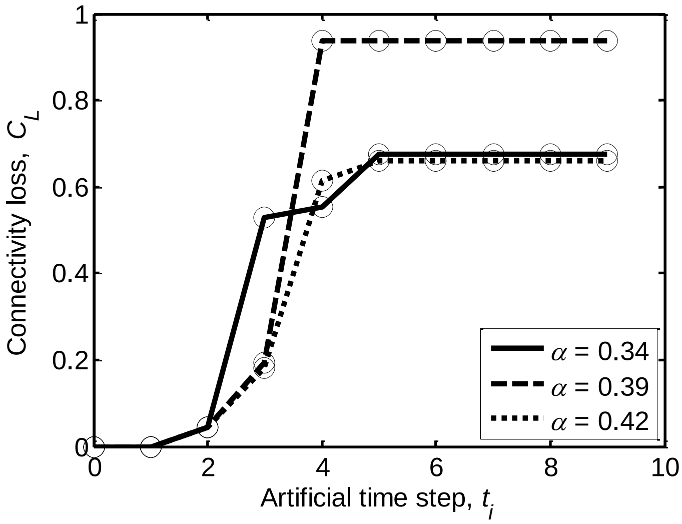

Figure 4. The cascade evolution in terms of the connectivity loss, C_L, for three values of the tolerance parameter in the range $0.34 \leq \alpha \leq 0.42$.

The C_L versus α curve of Figure 2 is relevant for safety, because it identifies the transition between the cascade-safe region and the onset of disrupting cascades in terms of the operating safety margin, α. As an example, in order to reduce the connectivity loss C_L below 60%, the power transmission network must be operated accounting for a safety margin $\alpha \geq$ 69% beyond the actual working load; the cascading failures occurring beyond this safety margin would result in connectivity losses lower than the selected value. Yet, such a wide safety margin might not be always available in real power transmission systems and component replacements might be required to comply with the prescribed safety margins. Information concerning the benefits of possible system improvements can also be inferred from the same curve. As an example, an increase in tolerance from α = 0% to α = 34% leads to a decrease in C_L; yet, the resilience to cascading failure does not benefit from further tolerance increments until a value α = 65% is reached. Furthermore, increasing α from 73% to 123% has no advantage at all. Hence, it cannot be said that simply increasing the tolerance α is an actual improvement for the system vulnerability towards cascading failures.

With respect to the malicious targeted attack of single nodes, the components of the system can be ranked in view of the damage caused by the cascade of failures triggered by their individual removal. To this aim, in Figure 5 the histogram of the connectivity loss, C_L, caused by the removal of each node in the power transmission system is presented for α = 30% which is a reasonable assumption in standard practice. Surprisingly, the most congested node {88} is not among the most critical. Nodes {14, 79, 76, 71 and 83} are ranked as the most critical ones, being bottlenecks for many generator-distributor shortest paths due to their position in the network. Hence, an attacker aiming at disrupting the most 'active' node would not actually produce the maximum 'desirable' damage.

The ranking of the most critical components is dependent on the tolerance parameter, α, characteristic of the system; thus it must be reevaluated in case the system undergoes modifications affecting its operating margins.

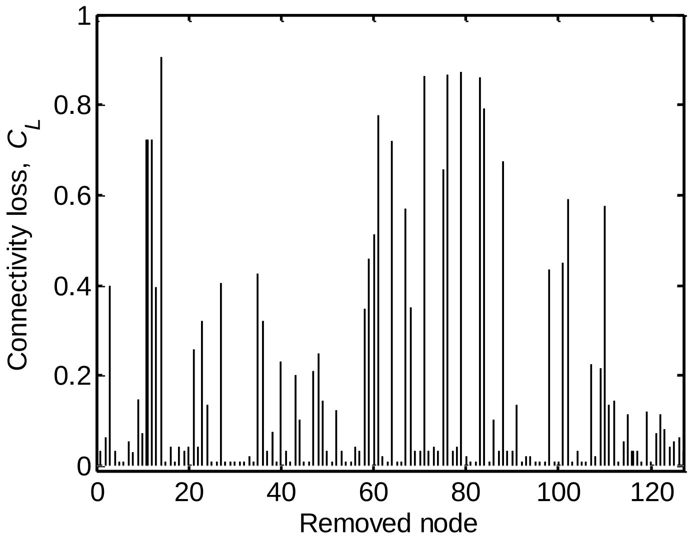

Figure 5. The connectivity loss, C_L, caused by the removal of each node (abscissa) in the power transmission system. The tolerance parameter is α = 30%.

5.2 *Interdependent CIs*

Two additional CIs interdependent on the power transmission network are considered, i.e. the communication network and the railway network; their local interaction rules have been detailed in Section 4.

The effects of the disconnection of the most congested node {88} in the power transmission on the communication and railway networks are reported in Figure 6, where the loss of service in terms of the relative decrease of the average global efficiency, ΔE_{glob}, with respect to the unperturbed systems is plotted versus the tolerance parameter α. Due to the strong physical interdependencies between the power transmission system and the two interdependent CIs, the loss of service trend is closely related to the connectivity loss, C_L, as it can be seen comparing Figure 2 and Figure 6. The evaluation of average indicators is not needed for this scenario, since the probabilistic cyber interdependencies act on nodes which have already failed due to the physical interdependencies from the power transmission system. Due to the higher degree of redundancy in the communication network, the loss of service for this infrastructure is smaller than it is for the railway system. The curve in Figure 6 provides vulnerability information as the one in Figure 2. As an example, if a designer aims at protecting the railway systems requiring a maximum loss of service, e.g. $\Delta E_{glob} \leq 0.5$, the interdependent power transmission network must be operated at $\alpha \geq$ 69%. From this curve, information on the feasibility and the benefits of power transmission system improvements can also be inferred with respect to the attainable reduction in the vulnerability of the interdependent CIs.

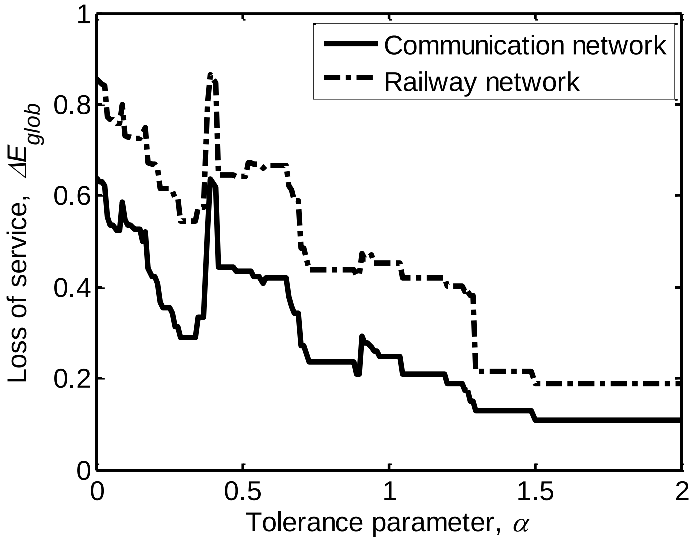

Figure 6. The loss of service in terms of the relative decrease of the average global efficiency with respect to the unperturbed systems vs. the tolerance parameter α. The cascades are triggered by the removal of the most congested node {88} in the power transmission system.

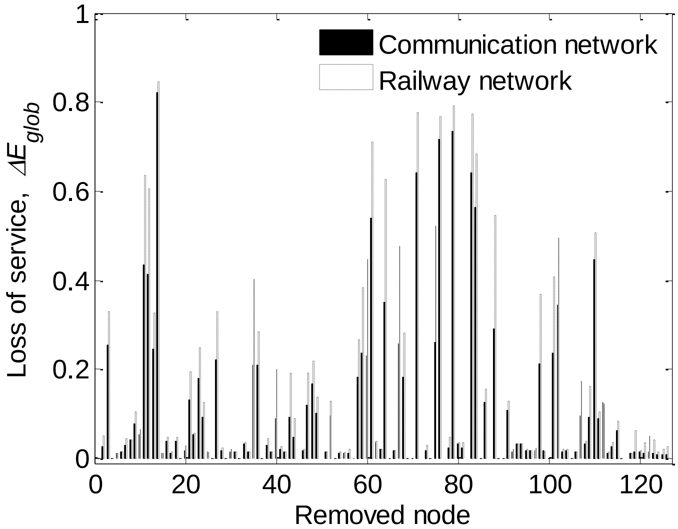

Figure 7. The loss of service, ΔE_{glob}, caused by the removal of each node (abscissa) in the power transmission system. The tolerance parameter is α = 30%.

In Figure 7, the removal of each node in the power transmission system is associated with its consequences on the interdependent CIs. Similarities with Figure 5 appear, for the reasons explained above.

Henceforth, the focus of the analysis becomes that of assessing the effects the intentional removal of the most connected node {88} belonging to the communication system. They are reported in Figures 7 and 8 as C_L and ΔE_{glob} vs. α, respectively, for the values of the interdependency strengths $p_{cr} = p_{cp}$ = 0.5. Comparing Figures 8 and 9 and Figures 2 and 6, it appears that cyber dependencies are less critical than physical dependencies with respect to the failure propagation, due to their assumed probabilistic nature.

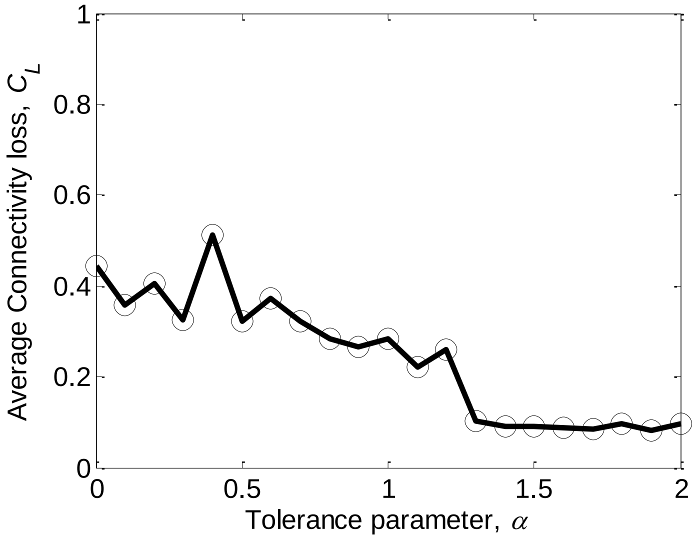

Figure 8. The final value of the connectivity loss, C_L, vs. the tolerance parameter, α. The results are averaged over 100 cascades triggered by the removal of the most connected node {88} in the communication system. $p_{cr} = p_{cp}$ = 0.5.

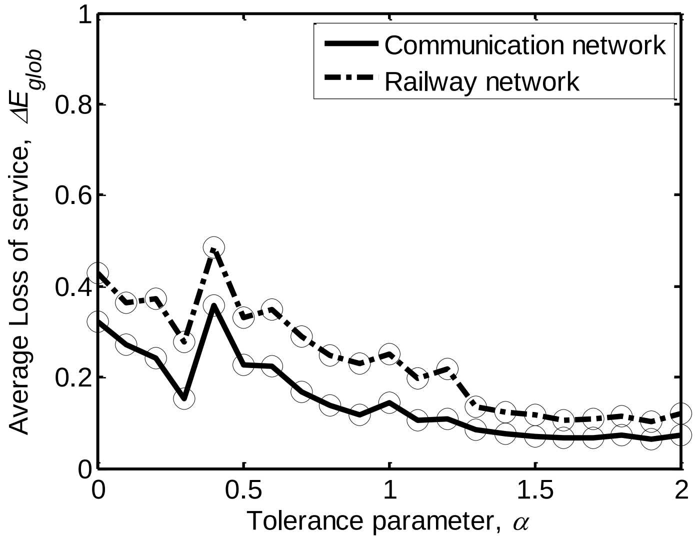

Figure 9. The loss of service, ΔE_{glob}, vs. the tolerance parameter α. The results are averaged over 100 cascades triggered by the removal of the most connected node {88} in the communication system. $p_{cr} = p_{cp}$ = 0.5.

Aiming at assessing the effects of the interdependency strengths on the failure propagation, a sensitivity study is carried out with respect to p_{cp} for two different α values and its results are reported in Figures 10 and 11, when p_{cr} = 0.5. A linear decrease is attained in the effects of the cascading failure in terms of C_L and ΔE_{glob} when the interdependency strength, p_{cp}, is reduced. Furthermore, the 'system-of-systems' sensitivity to p_{cp} decreases when the tolerance α increases, as indicated by the reduced slope for the case α = 30%. The curves in Figures 10 and 11 convey information concerning the vulnerability of CIs with respect to the interdependency strength. As an example, if a maximum service loss is prescribed for the railway system, e.g. $\Delta E_{glob} \leq$ 40%, the interdependencies between the communication system and the power system must be operated so that $p_{cp} \leq$ 70%.

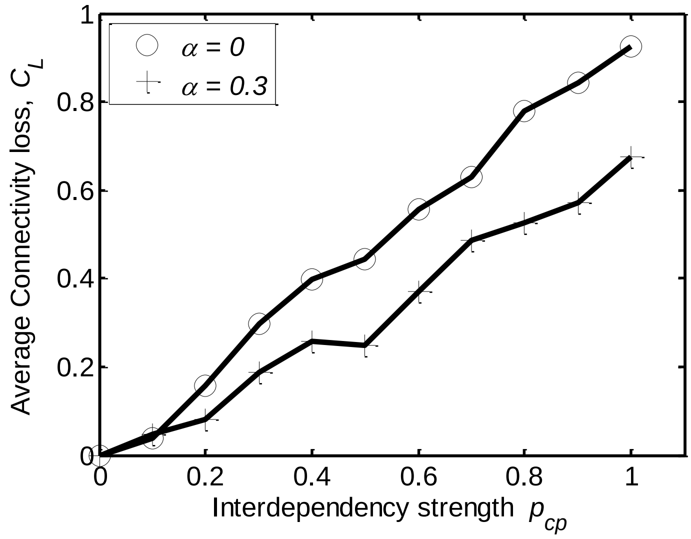

Figure 10. The connectivity loss, C_L, vs. the interdependency strength, p_{cp}. The results are averaged over 100 cascades triggered by the removal of the most connected node {88} in the communication system. p_{cr} = 0.5.

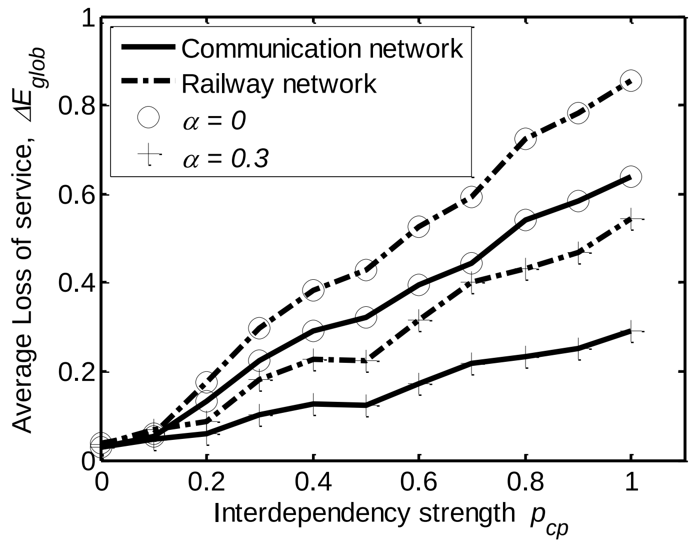

Figure 11. The loss of service, ΔE_{glob}, vs. the interdependency strength, p_{cp}. The results are averaged over 100 cascades triggered by the removal of the most connected node {88} in the communication system. p_{cr} = 0.5.

The interdependent CIs are not sensitive to variations of p_{cr}, which do not influence the cascade triggering in the power system.

Finally, the removal of each node in the communication system is associated with its consequences on the interdependent CIs in Figures 12 and 13. Similarly to the independent power transmission network case, the more connected node {88} in the communication system is not the most critical with respect to failure propagation (it is ranked lower that 13th for all the three CIs). Nodes {76, 14, 12 and 71} are ranked as the most critical for all the three CIs. Compared to the single infrastructure case of Section 5.1, the relative ranking of some node originally present has changed (i.e. nodes {14, 76 and 71}) and other nodes (i.e. node {12}) appear among the most critical.

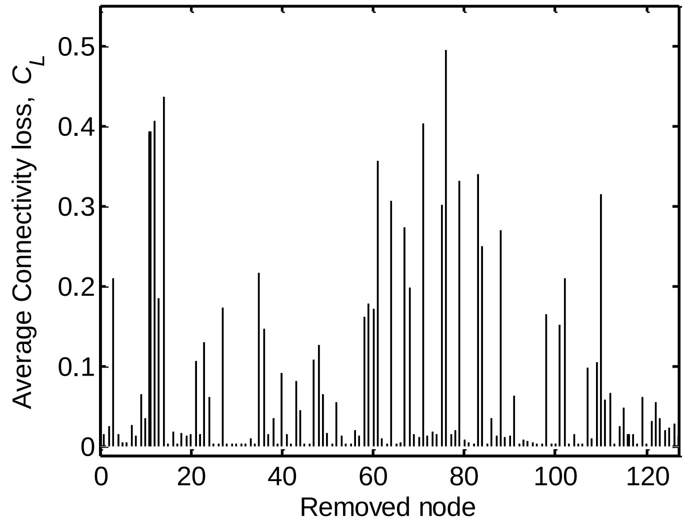

Figure 12. The average connectivity loss, C_L, caused by removal of each node (abscissa) in the communication system (100 simulations for each node). α = 30%, $p_{cr} = p_{cp}$ = 0.5.

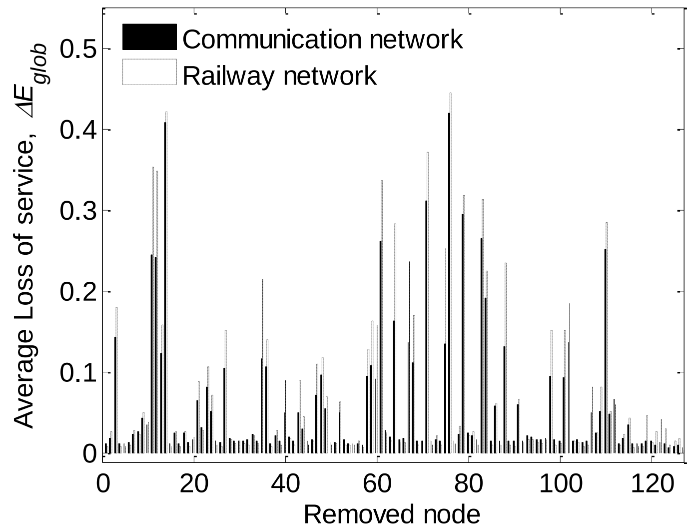

Figure 13. The loss of service, ΔE_{glob}, caused by removal of each node (abscissa) in the communication system (100 simulations for each node). α = 30%, $p_{cr} = p_{cp}$ = 0.5.

6 CONCLUSIONS

In an effort to enhance the capability of models of cascading failures propagation based on network theory, the physical characterization of components in a power transmission network and of interdependencies among CIs has been introduced. The model has been applied to assess the cascade propagation process triggered by a defined scenario: the malevolent targeted removal of single nodes. Three interdependent CIs have been considered, namely the power transmission network, the communication network and the railway network.

For the independent power transmission network case and the interdependent CIs case, the effects of the variations of the operating safety margin, α, on the cascade propagation have been assessed. The knowledge gained from this analysis can help setting the value of the operating safety margin, α, so as to limit the consequences of cascading failures, e.g. measured by C_L or ΔE_{glob}, in the CI.

Ranking of the nodes according to the disruptions triggered by their individual removal has shown that nodes which could be thought as most critical because of their high congestion or connectivity, are not associated with the largest consequences following their removal. This points to the fact that the physical characterization of the components and interdependencies adds a further level of complexity to the cascade propagation, so that the system bottlenecks cannot be identified though the static topological analysis alone but they require dynamical simulations.

The analyses performed confirm the need for early disconnection or islanding, through inclusion of 'weak' nodes in the system design.

For the interdependent CIs case, the extent to which the interdependency parameter, i.e. the interdependency strength, affects the cascade propagation has been assessed for various operating safety margins, α. Once the operating safety margin is known, the systems can be designed or operated, tweaking the interdependency strength, p_{cr}, to limit the maximum average connectivity loss, C_L or service loss, ΔE_{glob}.

Future developments of this work will be the modeling of active safety systems for preventing and mitigating cascading failures propagations and the analysis of interdependent CIs having their own individual cascade dynamics.

ACKNOWLEDGMENTS

This work has been partially funded by the Foundation pour une Culture de Securite Industrielle of Toulouse, France, under the research contract AO2006-01.

REFERENCES

Albert, R., H. Jeong, et al. 2000. Error and attack tolerance of complex networks. *Nature* 406(6794): 378-382.

Albert et al. 2004. Structural vulnerability of the North American power grid, *Physical Review E* 69, 025103.

Batagelj, V. 1994. Semirings for social networks analysis. *Journal of Mathematical Sociology* 19(1): 53-68.

Dobson, I., B. A. Carreras, et al. 2007. Complex systems analysis of series of blackouts: Cascading failure, critical points, and self-organization. *Chaos: An Interdisciplinary Journal of Nonlinear Science* 17(2): 026103.

Duenas-Osorio & Vemuru 2009. Cascading failures in complex infrastructures systems. *Structural safety* 31: 157-167.

Freeman, L. C. 1978. Centrality in social networks conceptual clarification. *Social Networks* 1(3): 215-239.

Freeman, L. C., S. P. Borgatti, et al. 1991. Centrality in valued graphs: A measure of betweenness based on network flow. *Social Networks* 13(2): 141-154.

Johansson and Jonsson 2009. A model for vulnerability analysis of interdependent infrastructure networks. *Safety, Reliability and Risk Analysis: Theory, Methods and Applications* – Martorell et al. (eds), Proceedings of ESREL 2008 and 17th SRA Europe Annual Conference, 22-25 September 2008, Valencia, Spain, Taylor & Francis Group, London, 2009.

Latora and Marchiori 2005. Vulnerability and protection of infrastructure networks. *Physical Review E* 71, 015103.

Little, R. G. 2002. Controlling Cascading Failure: Understanding the Vulnerabilities of Interconnected Infrastructures. *Journal of Urban Technology* 9(1): 109 - 123.

McDaniels, T., Chang, S., Peterson, K., Mikawoz, J. & Reed, D. 2007. Empirical Framework for Characterizing Infrastructure Failure Interdependencies. *Journal of Infrastructure Systems* 13(3): 175–184.

Motter, A. E. and Y.-C. Lai 2002. Cascade-based attacks on complex networks. *Physical Review E* 66(6): 065102.

Newman, M. E. J. and M. Girvan 2004. Finding and evaluating community structure in networks. *Physical Review E* 69(2): 026113.

Newman D. E. et al. 2005. Risk Assessment in Complex Interacting Infrastructure Systems, *Proceedings of the Thirty-Eight Annual Hawaii International Conference on System Sciences*, January 3-6, 2005, Computer Society Press.

Nieminen, J. 1974. On the centrality in a graph. *Scandinavian Journal of Psychology* 15(1): 332-336.

Rinaldi, S.M. et al. 2001. Identifying, understanding and analyzing critical infrastructures interdependencies, *IEEE Control System Magazine*, 21(6), 11-25.

Rinaldi, S.M. 2004. Modeling and simulating critical infrastructures and their interdependencies, *Proceedings of the Thirty-Seventh Annual Hawaii International Conference on System Sciences*, January 5-8, 2004, Computer Society Press.

Rosato, V., Bologna, et al. 2007. Topological properties of high-voltage electrical transmission networks. *Electric Power Systems Research* 77: 99-105.

Sabidussi, G. 1966. The centrality index of graphs. *Psychometrika* 31(4): 581-603.

TERNA. 2002. Dati statistici sull'energia elettrica in Italia. Techical Report. *Terna S.p.A. - Rete Elettrica Nazionale*. (in Italian) http://www.terna.it/LinkClick.aspx?fileticket=PUvAU57MlBY%3d&tabid=418&mid=2501

Zimmerman, R. 2001. Social Implications of Infrastructure Network Interactions, *Journal of Urban Technology*, 8(3): 97-119.

Zio, E. and G. Sansavini 2009. Modeling failure cascade in network systems due to distributed random disturbances. *Proceedings ESREL 2008. Martorell et al. (eds): Safety, Reliability and Risk Analysis: Theory, Methods and Applications.* CRC Press, Taylor & Francis Group, London.

Zio, E. and Sansavini, G. 2010. Modeling interdependent network systems for identifying cascade-safe operating margins, submitted to *IEEE Transactions on Reliability*, Special issue on Complex Systems.